



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/996,923	11/30/2001	Shoji Fukutomi	216642US8	3249
22850	7590	03/17/2005	EXAMINER	
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			HENNING, MATTHEW T	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 03/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/996,923

Applicant(s)

FUKUTOMI ET AL.

Examiner

Matthew T Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 30 November 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☒ Claim(s) 11 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

This action is in response to the communication filed on 11/30/2001.

**DETAILED ACTION**

1. Claims 1-18 have been examined.

***Title***

2. The title of the invention is acceptable.

***Priority***

3. The application has been filed under Title 35 U.S.C §119, claiming priority to Japanese application 2000-381042 filed December 14, 2000, and Japanese application 2001-139288 filed May 9, 2001..

4. The effective filing date for the subject matter defined in the pending claims in this application is December 14, 2000.

***Drawings***

5. The drawings filed on 11/30/2001 are acceptable for examination proceedings.

***Specification***

6. The disclosure is objected to because of the following informalities:

Page 18 Line 11 recites "DCHP" but should read "DHCP".

Page 11 Line 20, as well as many other places throughout the specification, recite "Diffie-Helman", but should recite "Diffie-Hellman".

Appropriate correction is required.

***Claim Objections***

7. Claim 11 is objected to because of the following informalities: Line 3 recites "Diffie-Helman" which should read "Diffie-Hellman". Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

*A person shall be entitled to a patent unless –*

*(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*

9. Claims 1, 6, 11, 13-14, and 16-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Aziz et al. ("Privacy and Authentication for Wireless Local Area Networks") hereinafter referred to as Aziz.

10. Regarding claim 1, Aziz disclosed a session shared key sharing method of sharing a session shared key for privacy and/or authentication between wireless terminal that transmits and receives a packet and a base station device that relays the packet when said wireless terminal and said base station device communicate with each other over wireless (See Aziz Abstract and Fig. 3), the method comprising: a first insertion step of inserting first information used for creating the session shared key into the packet transmitted from said wireless terminal to said base station device based on a protocol executed when said wireless terminal and said base station device start communicating with each other (See Aziz Page 8 Lines 8-10); a second insertion step of inserting second information used for creating the session shared key into the packet transmitted from said base station device to said wireless terminal based on the protocol (See Aziz page 8 Lines 11-12); a first creation step of allowing said base station device to create the session shared key based on the first information inserted in the first insertion step (See Aziz Page 8 Lines 13-21); a second creation step of allowing said wireless terminal side to create the session shared

Art Unit: 2131

key based on the second information inserted in the second insertion step (See Aziz Page 8 Lines 13-21).

11. Claim 6 is rejected for the same reasons as claim 1 above, and further because Aziz disclosed an encryption step of enciphering first information for creating a session shared key used for the authentication using a secret key (See Aziz Page 8 Lines 8-10 and Page 4 Line 2); and a decoding step of allowing said base station device transmit the enciphered first information inserted in the first insertion step authentication station decoding and resending information enciphered using the secret key, and to receive the first information decoded by the authentication station (See Aziz Page 8 Lines 8-10 and Page 5 Line 41 – Page 6 Line 1).

12. Regarding claim 11, Aziz disclosed that the first information and the second information are public keys based on a Diffie-Hellman type public key delivery method (See Aziz Page 8 Lines 8-12); and the session shared key is a shared key based on the Diffie-Hellman type public key delivery method (See Aziz Page 8 Lines 8-13).

13. Regarding claim 13, see the rejection of claim 1 above.

14. Regarding claim 14, see the rejection of claim 6 above.

15. Regarding claim 16, see the rejection of claim 1 above.

16. Regarding claim 17, see the rejection of claim 6 above.

### ***Claim Rejections - 35 USC § 103***

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

*(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole*

Art Unit: 2131

*would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.*

18. Claims 2, 4-5, 7, and 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz as applied to claims 1 and 6 above, and further in view of Murakawa (US Patent Application Publication 2001/0020273).

Regarding claims 5 and 10, Aziz disclosed a system for exchanging keys and authentication information between a mobile device and a base station a connection time (See Aziz Page 4 Secure Protocol Description Line 1), but Aziz failed to disclose the DHCP protocol being a part of the key exchange protocol.

Murakawa teaches that the DHCP protocol can be integrated into a key exchange protocol in order to provide the client with an IP address (See Murakawa Paragraph 0044).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakawa in the key exchange system of Aziz by integrating the DHCP protocol in the key exchange protocol. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the mobile terminal to communicate within the LAN by virtually regarding it as another terminal on the LAN.

19. Regarding claims 2 and 7, the DHCP protocol provides a network layer address to the client (See Murakawa Paragraph 0044).

20. Regarding claims 4 and 9, the DHCP protocol provides an IP address (See Murakawa Paragraph 0044), which corresponds to a MAC address.

Art Unit: 2131

21. Claims 3 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Aziz and Murakawa as applied to claims 1 and 6 above, and further in view of Massarani (US Patent Number 6,393,484).

The combination of Aziz and Murakawa disclosed a system for exchanging keys between a wireless device and an access node, and for providing the wireless device with an IP address (See the rejection of claim 5 above), but failed to specifically disclose the key exchange and IP assigning further including an address resolution protocol.

Massarani teaches that when an IP address is assigned to a device through DHCP, the address resolution protocol updates the MAC table with the IP address and MAC address correlation (See Massarani Col. 3 Lines 47-57).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Massarani in the Key and IP exchange protocol of Aziz and Murakawa by having the ARP update the MAC table of the access point when the IP address was assigned to the wireless device. This would have been obvious because the ordinary person skilled in the art would have been motivated to keep track of the IP addresses in the LAN, as well as the devices using them.

22. Claims 12, 15, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz as applied to claims 6, 14, and 17 above, and further in view of Friedman et al. (US Patent Number 6,240,513) hereinafter referred to as Friedman, and further in view of Schneier (Applied Cryptography), and further in view of Sato (US Patent Number 5,592,468).

Aziz disclosed encrypting the packets with the exchanged key (See Aziz Page 7 Lines 35-36), a first CRC value calculation step of calculating a CRC value based on data including the

Art Unit: 2131

payload of the packet and the hash value calculated in the first hash value calculation step (See Aziz Page 7 Lines 35-36); and a packet transmission step of transmitting the packet with the CRC value calculated in the first value calculation step being added to the MAC header and the payload of the packet, from said wireless terminal said base station device (See Aziz Page 7 Lines 35-36); but Aziz failed to disclose a first hash value calculation step calculating a hash value based on data including a data link layer payload of the packet transmitted from said wireless terminal said base station device and the session shared key created in the second creation step; the CRC data including the MAC header; a second hash value calculation step of allowing said base station device to calculate a hash value based on data including the MAC header and the payload transmitted in the packet transmission step and the session shared key created first creation step; a second CRC value calculation step of calculating a CRC value based on data including the MAC header and the payload transmitted in the packet transmission step and the hash value calculated in the second hash value calculation step; and an authentication step of allowing said base station device to authenticate said wireless terminal for each packet comparing CRC value transmitted the packet transmission step with the CRC value calculated in the second CRC value calculation step.

Friedman teaches that by hashing a packet and then encrypting the hash, the packet and the sender can be authenticated (See Col. 16 Lines 28-36).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Friedman in the communication system of Aziz by hashing the encrypted packets to create a digital signature for each packet. This would have been



Art Unit: 2131

obvious because the ordinary person skilled in the art would have been motivated to provide authentication of the packets.

Schneier teaches that in order to verify the authenticity of a hash signature, the receiver must recalculate the hash (See Schneier Page 38 Lines 34-37).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the communication system of Aziz and Friedman by recalculating the hash of the received packet at the base station in order to check the authenticity of the packet.

Sato teaches that MAC packets have a CRC attached to the header and the body and that they are used to detect errors in transmission (See Sato Col 13 Lines 42-55).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Sato in the communication system of Aziz, Friedman and Schneier by including the CRC of the data, including the hash which is part of the IP packet, in the CRC, as well as recalculating the CRC upon receipt of the packet at the base station. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide assurance that there were no errors in the transmission of the packets.

### *Conclusion*


23. Claims 1-18 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.


Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Matthew Henning  
Assistant Examiner  
Art Unit 2131

3/10/05

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100